

id: 165612
date: 8/11/2008 16:10
refid: 08RIYADH1230
origin: Embassy Riyadh
classification: SECRET
destination:
header:
VZCZCXYZ0009
OO RUEHWEB

DE RUEHRH #1230/01 2241610
ZNY SSSSS ZZH
O 111610Z AUG 08
FM AMEMBASSY RIYADH
TO RUEHC/SECSTATE WASHDC IMMEDIATE 8948
INFO RUEHJI/AMCONSUL JEDDAH IMMEDIATE 9673
RUEHRH/CHUSMTM RIYADH SA IMMEDIATE
RUEAIIA/CIA WASHDC IMMEDIATE
RHMFISS/COMUSCENTAF SHAW AFB SC IMMEDIATE
RHRMAKS/COMUSNAVCENT IMMEDIATE
RHEBAAA/DEPT OF ENERGY WASHINGTON DC IMMEDIATE
RUEAUSA/DEPT OF HHS WASHDC IMMEDIATE
RUEATRS/DEPT OF TREASURY WASHDC IMMEDIATE
RUEKDIA/DIA WASHINGTON DC IMMEDIATE
RUEAHLA/HOMELAND SECURITY CENTER WASHINGTON DC IMMEDIATE 0235
RHMFISS/HQ USCENCOM MACDILL AFB FL IMMEDIATE
RHEHNSC/NSC WASHDC IMMEDIATE
RUEKJCS/SECDEF WASHDC IMMEDIATE
RHEHAAA/WHITE HOUSE WASHINGTON DC IMMEDIATE

----- header ends -----

S E C R E T RIYADH 001230

SIPDIS

DEPARTMENT FOR NEA/ARP, S/CT, AND PM
WHITE HOUSE FOR OVP

E.O. 12958: DECL: 08/10/2018
TAGS: ECON, ENRG, EPET, PGOV, PINR, PREL, PTER, SA
SUBJECT: CRITICAL INFRASTRUCTURE PROTECTION IN SAUDI: NEXT
STEPS

Classified By: Charge' d'Affaires Michael Gfoeller
for reasons 1.4 (B) and (D)

1. (S) SUMMARY. The enormous Saudi energy facilities located in the Kingdom's Eastern Province, which provide approximately 12 percent of global oil supply, remain highly vulnerable to external attack. Even partial disruption of these production facilities would have an immediate impact on oil supplies and prices, with a likely devastating impact on the U.S. national economy and the global economy as a whole.

The Technical Cooperation Agreement (TCA) on Critical Infrastructure Protection (CIP) signed at the US-Saudi Summit Meeting in May by the Secretary and Saudi Interior Minister Prince Nayif bin Abd al-Aziz created a Joint Commission to oversee bilateral cooperation in implementing CIP. Developing and implementing the Joint Commission's technical work program is a foremost priority to ensure the production and supply of Saudi oil is secure from terrorist attack. As we move to stand up the Joint Commission, Embassy Riyadh proposes the attached substantive work plan for the next 12-18 months, which Saudi Ministry of Interior (MOI) interlocutors have confirmed corresponds to their priorities. In addition, we should also make progress on setting up the management and financial structure of the Joint Commission, without which the substantive work program cannot move forward swiftly and efficiently. END SUMMARY.

CONTINGENCY PLANNING

2. (S) Background: During President Bush's May 2008 visit to the Kingdom, Secretary Rice signed the Technical Cooperation Agreement authorizing the formation of the Joint Commission on Infrastructure and Border Protection. Developing and implementing the Commission's technical work program is a foremost priority to ensure the supply of Saudi oil is secure from attack. The Saudi Ministry of Interior's (MOI) first priority for the existing Joint Working Group (JWG) on Critical Infrastructure Protection (CIP) and the new Joint Commission on Infrastructure and Border Protection is completing work on contingency planning for key critical infrastructure facilities. The MOI is deeply concerned about possible attacks on these facilities by Al-Qaeda or other terrorist networks, whether domestic or international, or by hostile neighbors, particularly Iran.

3. (S) This contingency planning provides for systematic study, planning, and regular exercising - before a catastrophic attack - to ensure resiliency of capability and operations. It provides for designing system redundancy ahead of time, and planning for both government and company measures which allow maximum recoverability of operations in the fastest possible period of time. Proper contingency planning mitigates the worst consequences of an attack. Together with proper security measures, contingency planning provides for continuity of business and operations under extreme conditions.

4. (S) So far, the Joint Working Group (JWG) on Critical Infrastructure Protection (CIP) and a select inter-agency team have completed a review of a number of existing Saudi contingency plans, including those from Saudi Aramco, SABIC (petrochemical), SWEC (water), SEC

(power), the Royal Commissions of Yanbu and Jubail (integrated industrial cities), and Civil Defense, a department within MOI (civil response). The plans were generally found to be less than credible, given high terrorism and transnational threats to key installations. The Saudi Aramco plans were better developed than some of the others. Yet while

the plans were of superior quality, they do not appear to be regularly exercised, so the assessors remain doubtful they could be implemented to a high standard.

5. (S) In our JWG meetings to date with the MOI, we have explained the U.S. government-industry partnership model for contingency planning - we coordinate jointly, and engage in regular crisis simulations and exercises together to practice this cooperation. We noted the USG is responsible for continuity and response plans, while industry is responsible for continuity of operations and recovery plans.

PROPOSED NEXT STEPS IN CONTINGENCY PLANNING

6. (S) The next steps include conducting a gap analysis of the existing Saudi contingency plans, carrying out mitigation planning, and working with the MOI and the Saudi parastatal firms (e.g., Saudi Aramco, SABIC, SEC, SWEC) to develop generally more robust contingency planning documents. Finally, we should work with the MOI and these parastatal firms to conduct table top exercises, and eventually, full-scale crisis simulations. The annual planning and exercise cycles should be followed by comprehensive plan reviews. In the future, this work may be coordinated through the JWG on CIP, as well as the newly-established Joint Working Group on Homeland Security.

7. (S) The completion of vulnerability assessments, as noted below, should proceed simultaneously, as this work will provide additional engineering and security knowledge for the contingency planning.

VULNERABILITY ASSESSMENT OF OIL FACILITIES

8. (S) We have worked with the Ministry of Interior since 2006 to identify the Kingdom's most critical infrastructure and assess its vulnerabilities. We have provided preliminary security recommendations to defend several of the most important energy installations, including Abqaiq, Qateef Junction, Ras Tanura, and the Royal Commission cities of Jubail and Yanbu. However, in light of the increasing threat facing these facilities, the paradigm has changed. We are now

moving to apply in Saudi Arabia the same model we use to protect nuclear facilities internationally - a highly-rigorous, mathematical, and engineering-based model. This model is named Design-Based Threat (DBT), which has been presented to the Kingdom by Sandia National Laboratories under the direction of the Department of Energy. Sandia has provided similar training to forces protecting nuclear facilities all over the world where the USG deems it in our strategic national interest.

9. (S) In June 2007, under the direction of a technical team from Sandia Labs, a twenty-two person security team composed of officials from the Ministry of Interior, and security officials from Saudi Aramco, SABIC, SEC, and SWEC (the energy, petrochemical, power and water sectors) completed a ranking of the Kingdom's most important critical infrastructure. Facilities were ranked as Tier I, II, and III according to their criticality to the Kingdom and world. The Sandia team also provided associated training to these officials on threat-based design and improving security at individual installations.

10. (S) Training included identifying internal and external threats (also domestic vs. international),

the motivations, intentions and capabilities of these threats (group size, weapons, explosives, tools, transport, skills, funding, collusion, etc.), collecting and organizing threat-related information, formalizing threat-related information, defining a threat-based design from the threat assessment, and introducing the threat-based design into the national regulatory framework.

PROPOSED NEXT STEPS IN VULNERABILITY ASSESSMENT

11. (S) In order to understand the vulnerabilities of the Kingdom's infrastructure at an in-depth level, we must move from the 2-3 day "walk-the-fence" security overviews we have conducted in the past. We used these overviews to provide useful but preliminary security recommendations to the MOI.

12. (S) The Vulnerability Assessment (VA) is an in-depth, technical review of the facility's operational and security systems. The VA includes a 2-week on-site data collection and discussion period, followed by a month-long data analysis period. The Saudi MOI would receive VA results and recommendations within about one month after completion of the on-site data collection in Saudi Arabia. We are particularly concerned to identify Abqaiq components which were custom-manufactured several decades ago, in the 1970s, and for which Saudi Aramco may have no replacements or spare parts. Such

single-point failures would be of grave concern.

13. (S) The assessment of Abqaiq Plants, the Kingdom's most critical facility, is currently ongoing and will be completed by late August, 2008. An in-depth analysis of Abqaiq's engineering plans and drawings, along with extended access to and discussion with key technical personnel, are being done to better understand the plant's specific vulnerabilities. The Saudis' willingness to share this level of technical detail with us on the world's most important petroleum facility is unprecedented in our relationship. Only two successive Presidential visits and the signing of the TCA could have made this level of cooperation possible.

14. (S) After conducting the VA of Abqaiq, we recommend the next move be a similar assessment of the Ras Tanura Complex. Ras Tanura is Saudi Arabia's largest crude oil export facility, and includes export facilities, tank farms, Sea Island crude loading facility, a refinery, and a host of other associated facilities. Ras Tanura can export more than 5 million-plus barrels/day of crude, and should be the USG's next facility of major concern. A VA of Ras Tanura will be several orders of magnitude more complex than Abqaiq, as the complex is vast, over 10 kilometers long, and includes both land-based and maritime facilities. In spite of these difficulties, given Ras Tanura's role in crude exports, conducting a VA of Ras Tanura is key to USG interests.

15. (S) After conducting VAs of these two facilities, we should engage the MOI in discussions regarding the next target for a VA, using a list of Tier I facilities to guide our discussions. The next target facility could be a major desalination or power plant, which may not meet specific USG interests. However, the Saudi government could view such facilities as critical to its ability to sustain essential services to its population. We may wish to propose a VA of the Jubail Desalinization Plant (second on the Saudi's list of critical infrastructure after Abqaiq), an argument which likely find favor with the Saudi government. The

Jubail Desalinization Plant provides Riyadh with over 90% of its drinking water. Riyadh would have to evacuate within a week if the plant, its pipelines, or associated power infrastructure were seriously damaged or destroyed. The current structure of the Saudi government could not exist without the Jubail Desalinization Plant.

16. (S) Future work on VA issues should be coordinated through the JWG on CIP, as well as the newly-established Joint Working Groups on Ports and Oil Terminals, and JWG on Coast Guard.

NATIONAL THREAT NOTIFICATION SYSTEM PLANNING

17. (S) Saudi Arabia currently has no coordinated, national threat notification system. Individual firms, such as Saudi Aramco, do have threat warning systems. However, they are not coordinated or linked with a government security force threat warning system. Development of a national threat warning system is critical to the MOI's ability to protect critical infrastructure from terrorism or other threats, and to carry out robust civil response functions.

18. (S) During a July DOE delegation visit to Riyadh led by Assistant Secretary Kolevar, DOE Infrastructure System Analyst Vandermeij presented a brief to Saudi Joint Working Group Co-Chair Dr. Saud-Al Semari on the U.S. threat warning systems. She explained DHS's Homeland Security Advisory System and the U.S. Coast Guard Maritime Security System (MARSEC). Our MOI interlocutors were particularly impressed to learn how the USG works with industry in implementing the threat warning system, sharing information on an as-needed basis, and even sponsoring some industry personnel for security clearances so that information could be better shared. MOI, DOE, and Embassy interlocutors discussed the utility of restricting a specific threat warning to a given region, city, or industrial sector.

PROPOSED NEXT STEPS IN NATIONAL THREAT NOTIFICATION SYSTEM

19. (S) Dr. Saud-Al Semari requested the USG make available an employee who is familiar with the U.S. threat warning systems to assist the MOI in implementing a threat warning system for Saudi Arabia. DOE Assistant Secretary Kevin Kolevar offered DOE Infrastructure System Analyst Carissa Vandermay to provide initial guidance in August 2008. We are waiting for an MOI response to this offer, which we expect to be strongly positive. After these initial meetings, we should identify a USG expert, Vandermay if possible, for an additional 1-2 months in the Kingdom to further develop the national threat warning system. In the future, this work may be coordinated through the newly-established Joint Working Group on Homeland Security.

FACILITIES SECURITY FORCES TRAINING

20. (S) By 2007, the Saudi MOI had identified the Facilities Security Force (FSF) as the primary organization responsible for protecting the country's critical energy infrastructure. They determined the force would

be organized and trained for defensive and offensive missions in the protection of oil, gas, national power, and other sites that were heretofore under the protection of various branches of the MOI and MODA. Proposed civilian

nuclear power production facilities would also be under the FSF umbrella. MOI is in the process of recruiting and training an entirely new force of 35,000 personnel for this purpose. To date, over 10,000 new recruits have been put through initial training, with forces from the Ministry of Defense and Aviation (MODA) and the Saudi Arabian National Guard (SANG) reinforcing the FSF in its role until the FSF is fully staffed.

21. (S) Since the 2007 JWG discussions, the FSF has been a component of the JWG framework. FSF officers participated in the June 2007 workshop on threat analysis and contingency planning. Based on this training, in January 2008, a highly experienced group of Sandia trainers conducted an assessment of several FSF training centers, training doctrine, and courses. The Embassy's Defense Attach Office and Economic section also participated.

22. (S) The assessment provided MOI with recommendations on a number of key organizational changes to support the MOI's goal of rapidly expanding FSF manpower to assume security responsibilities. The assessment team recommended FSF quickly expand the Training Department, and separate it from the FSF Operations Unit. With this new emphasis on training, the training staff could recruit and train more instructors. They recommended a more rigorous process for selecting trainers with the appropriate background (much of the FSF instructor staff was taken from MOI and MODA units that are devoted to traditional combat arms, rather than facilities protection). The assessment team recommended FSF seek new training technology to improve the standard of training. Additionally, the assessment team encouraged MOI to fully support the establishment of a dedicated FSF academy and the expansion of FSF training facilities.

PROPOSED NEXT STEPS FOR FACILITIES SECURITY FORCES

23. (S) The FSF is rapidly assuming its role as a 35,000-plus man uniformed security force charged with defending Saudi Arabia's critical infrastructure. This includes defending Saudi Arabia's critical infrastructure against terrorist attack, and could include close cooperation and coordination with MODA and SANG in the event of an attack by a regional neighbor. A large training contract will be required to support the creation of the FSF, along the lines of what private contractors such as Vinnel do now under the auspices of the Office of the Program Manager - Saudi Arabian National Guard (OPM-SANG). However, even after

a training contract is signed with a suitable contractor, significant USG personnel assets would be necessary to support the creation and training of the FSF, and to advise its leadership.

24. (S) There seems to be a clear role for DOD and CENTCOM to play here. Training, equipment, and doctrine would all seem to be areas in which CENTCOM could bring a great deal to the table. The MOI is moving ahead swiftly to train the FSF, regardless of our involvement. They have already asked Pakistan and other forces to assist in this training during the past year, as we have been unable to respond quickly with further assistance. The nature of the Facilities Security Force's mission places it squarely in CENTCOM's area of responsibility (AOR). It seems advisable to expedite the USG efforts to train and equip the FSF, in order to assure this vital initiative remains within the purview of U.S.- Saudi security cooperation, instead of being subcontracted to a third state. DoD involvement, of course, is predicated upon obtaining the proper legal authorities.

CREATING A FINANCING PIPELINE

25. (S) The MOI has told us multiple times they are ready to pay nearly all the costs of CIP implementation. The CIP Agreement contains this Saudi commitment. An essential next step in this regard is the establishment of the necessary financial pipeline, which would consist of a bank account at the Federal Reserve, under the Treasury Department's supervision. One available option for this financing might be the old account once used by the US-Saudi Joint Economic Commission (JECOR), which still exists. Once we have the account established, MOI has promised to begin to fund CIP activities. CIP implementation should then progress quickly, while placing a minimal financial burden on the USG.

ESTABLISHING A CIP COORDINATOR POSITION

26. (S) CIP will be a complex undertaking. Proper implementation of this major initiative will require a dedicated, senior-level officer at post, operating under the authority of the Chief of Mission. Given the Saudis' sense of urgency regarding CIP and the very real nature of the threat from Iran and al-Qaeda to the Kingdom's energy sector, this position should be created and staffed as soon as possible. The incumbent would oversee all aspects of CIP implementation at post and deal on a daily basis with senior figures in the Saudi

government, especially the MOI, on CIP issues. The incumbent would also oversee all other personnel at post involved in CIP implementation.

AN HISTORIC OPPORTUNITY TO COUNTER A MAJOR THREAT

27. (S) COMMENT AND RECOMMENDATION: The continuing vulnerability of Saudi Arabia's strategic oil and gas production facilities represents an Achilles' heel for US strategic interests in the Kingdom and the broader Gulf region, not to mention US economic security in general. In the estimation of the MOI, these facilities face a serious threat from both al-Qaeda and Iran. Al-Qaeda in fact attacked one of the Kingdom's key energy sector sites, the Abqaiq oil and gas separator, in February 2006. Describing the terrorists' failure in that assault, Prince Muhammad bin Naif remarked to the Charge', "We did not save Abqaiq, God did." Had the attack been successful, it could have reduced Saudi Arabia's oil production and export capacity severely, in addition to drastically impacting the Saudi gas industry. The effect on oil prices of a successful repeat attack on Abqaiq or another key energy sector site would be catastrophic. The Saudis realize this. Indeed, it was the psychological shock produced by the Abqaiq incident that first led the Saudis to consider creating the Facilities Security Force, begin CIP talks with the USG, and conclude the CIP Agreement with us this May.

28. (S) USG participation in CIP could offer us tremendous opportunities. CIP implementation has huge commercial potential, which could be measured in billions of dollars worth of contracts. More importantly, it would result in the largest expansion of USG influence in Saudi Arabia in a generation, via the creation of a qualitatively new relationship with the MOI. If we move quickly, we can seize this opportunity. If we wait too long, the Saudis could potentially decide to offer it to one of our competitors. Such a

development would lead to a permanent loss of US influence in this strategically vital country. We therefore recommend rapid implementation of the proposed CIP work plan, establishment of a CIP funding mechanism, and the creation and staffing of a senior-level CIP Coordinator position at Embassy Riyadh under the authority of the Chief of Mission.

END COMMENT AND RECOMMENDATION.

GFOELLER

=====CABLE ENDS=====